УДК 661.3.066

А. В. Шабров, Л. К. Бочарников
Научный руководитель: аспирант К. Л. Стойчин
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМА ИНТЕРВЬЮИРОВАНИЯ СОТРУДНИКОМ, ПРОВОДЯЩИМ ОБСЛЕДОВАНИЕ НА ОБЪЕКТЕ, ДЛЯ ПОЛУЧЕНИЯ ИСХОДНЫХ ДАННЫХ ДЛЯ ФОРМИРОВАНИЯ ДОКУМЕНТОВ

Аннотация. В статье рассмотрены актуальные вопросы взаимодействия аналитика компании, занимающейся организацией мероприятий по защитей информации на объектах компании-заказчика и пользователей этой компании.

Ключевые слова: обследование; персональные данные; правовое обеспечение информационной безопасности; интервьюирование.

Чтобы объяснить тематику данной проблемы, рассмотрим пример. Существует компания «Норма», деятельность которой подразумевает обработку персональных данных, таких как паспортные данные, ИНН, СНИЛС и фактический адрес проживания. Для того чтобы компания могла функционировать и, как следствие, получать прибыль, она обязана соответствовать ряду различных правил, соблюдать федеральные законы Российской Федерации, получать лицензии и многое другое. Безопасность персональных данных лежит в основе продолжения деятельности любого предприятия и компании, причиной этого являются Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который обязывает компанию, работающую с персональными данными, их защищать. В большинстве случаев компании не имеют условий для организации мероприятий по защите информации на своих объектах в соответствии с законодательством, по этой причине существуют фирмы, у которых есть право и средства для этого. Назовем эту фирму «Безопасность» и рассмотрим абстрактный вариант взаимодействия двух этих фирм:

1. «Норма» и «Безопасность» заключают контракт на предоставление услуги «Реализация проекта по защите информации на рабочих местах № 1, 2, 3, 4, 5».

2. На каждое из этих рабочих мест фирма «Безопасность» направляет специалистов — аналитика и инженера.

3. Аналитик производит обследование рабочего места для дальнейшей разработки пакета документов, проектировку рабочего места и перечня персональных данных, которые на этом рабочем месте обрабатываются.

4. Инженер устанавливает комплекс защитных средств (например, антивирусное программное обеспечение и систему защиты информации).

5. Фирме «Норма» передается пакет документов, подтверждающих соответствие критериям, которые выдвигает государство к рабочим местам, на которых обрабатываются персональные данные.

После рассмотрения краткого алгоритма взаимодействия компаний перейдем к основной теме данной статьи — взаимодействие аналитика из «Безопасности» и пользователей из компании «Норма». Рассмотрим еще один пример. Аналитик приходит (по предварительной договоренности) на рабочее место сотрудника и возникает следующая ситуация: аналитик представляется сотрудником фирмы «Безопасность» и говорит пользователю о необходимости провести обследования его рабочего места взять интервью по теме «Обработка персональных данных». Далее рассмотрим предпочтительный для сотрудника фирмы, предоставляющей услуги по обеспечению информационной безопасности, вариант — пользователь осведомлен о визите аналитика и подготовил перечень обрабатываемых персональных данных, список программного обеспечения, с помощью которого эти данные обрабатываются, перечень нормативных актов и федеральных законов, в соответствии с которыми эти данные обрабатываются, приветлив и знает о необходимости данного мероприятия. Соблюдение всех этих условий редко соответствует действительности, и специалист «Безопасности» сталкивается с рядом проблем, основными из них являются:

1. Пользователь не знает, зачем проводится данное мероприятие.
2. Пользователь не владеет понятиями информационной безопасности.
3. Пользователь не хочет идти на контакт.

При наличии данных проблем и всеми вытекающими из них последствиями проведение исследования и дальнейшей работы становится невозможным. Приведем основные варианты разрешения данных проблем:

1. Специалист сообщает пользователю о последствиях исполнения его работы без помощи пользователя, которые могут повлечь за собой ошибки в организации защиты, а следовательно, нарушения федерального законодательства. В свою очередь это повлечет ответственность фирмы «Норма», например Кодекс об административных правонарушениях дает возможность оштрафовать физическое или должностное лицо, индивидуального предпринимателя или компанию за невыполнение 152-ФЗ на 10 000 рублей. Штраф может быть наложен не только на компанию, но и на работника, руководителя или ответственного за организацию обработки персональных данных. Также компания может быть оштрафована на сумму до 20 000 рублей, если не выполнит в срок предписание Роскомнадзора или не ответит на его запрос. Данный способ эф-

фективен, но может дать обратный эффект, и пользователь может отказаться продолжать работу со специалистом.

2. Специалист обращается за помощью к непосредственному заказчику, куратору данного мероприятия на предприятии для дальнейшего общения с пользоваелем. Способ эффективен в случае, если обследования проводятся на небольшом объекте. Не всегда представляется возможность взаимодействовать с руководством пользователя постоянно.

Помимо предложенных методов, каждый специалист обычно имеет свои способы, которые не прописаны в регламентах фирм, представляющих подобные услуги.

Также для эффективного проведения обследования и интервьюирования в частности перед выходом на объект специалисту необходимо подготовится к данному мероприятию:

1) проанализировать деятельность и нормативную базу, по которой работает данное предприятие;

2) вывести предполагаемый список персональных данных, с которыми может работать пользователь, место которого предстоит исследовать на основании анализа предыдущего пункта;

3) составить анкету для пользователя;

4) если подобные предприятия или их отделы уже были обследованы ранее, возможно использовать готовую анкету с прошлых объектов;

5) направить руководителю предприятия письмо, содержащее перечень предстоящих мероприятий, когда они будут проводится, и вложить анкету с просьбой ознакомить пользователей с этой анкетой для предстоящей работы.

В настоящее время существует множество различных способов для интервьюирования пользователей, однако не существует оптимизированного подхода для решения возникающих в ходе выполнения поставленной задачи проблем, в связи с этим каждый специалист, проводящий обследования, вынужден самостоятельно разрабатывать методики и средства для эффективного выполнения своих рабочих обязанностей.

В результате данного исследования можно вывод о том, что необходимо на основе нормативно-правовой базы Российской Федерации разработать методические рекомендации, целью которых будет регламентированный универсальный метод взаимодействия с пользователем, в частности касающийся предоставления информации, которая относится к обработке информации. Следует отметить, что данный метод должен быть динамически изменяем в зависимости о применяемой нормативно-правовой базы, регламентирующей вопросы обработки персональных данных и особенностей обработки в зависимости от специфики нормативно-правовой базы, по которой работает объект с персональными данными.